Exhibit 300: Capital Asset Summary

Part I: Summary Information And Justification (All Capital Assets)

Section A: Overview & Summary Information

Date Investment First Submitted: 2010-03-17
Date of Last Change to Activities: 2012-02-27
Investment Auto Submission Date: 2012-02-27
Date of Last Investment Detail Update: 2012-02-27
Date of Last Exhibit 300A Update: 2012-07-23
Date of Last Revision: 2012-05-22

Agency: 009 - Department of Health and Human Services **Bureau:** 00 - Agency-Wide Activity

Investment Part Code: 02

Investment Category: 00 - Agency Investments

1. Name of this Investment: Secure One HHS

2. Unique Investment Identifier (UII): 009-000006779

Section B: Investment Detail

1. **Provide a brief summary of the investment, including a brief description of the related benefit to the mission delivery and management support areas, and the primary beneficiary(ies) of the investment. Include an explanation of any dependencies between this investment and other investments.**

Secure One HHS (HHS Cybersecurity Program), the Department's IT Security program, assists in meeting the challenge of protecting HHS' information and information resources. The program is championed to secure HHS' most critical assets (both cyber and physical), such as computer systems, networks, and Department laboratories. Secure One HHS uses program management, governance, and technology to promote sound security practices, support legislative compliance and meet business needs. It focuses on the development and implementation of IT security policy, procedures, and guidance which are promulgated through top down communications, awareness campaigns, and training. Secure One HHS is responsible for the procurement of commercial off-the-shelf (COTS) technology, such as Gideon and Watchfire, to monitor and scan its networks for vulnerabilities. The Program leverages Checkpoint to ensure the encryption of sensitive information and Personally Identifiable Information (PII). The Program employs contract support for Web Application Vulnerability Scanning System (WAVSS) which serves to identify, track, and report on the Department’s vulnerabilities for public and internal web-based applications and websites. Program software tool components, combined with program professional services support and a centralized Program management team, ensure a comprehensive, defense-in-depth security strategy. This investment supports efforts to increase its Federal Information Security Management Act (FISMA) score. The Program focuses priority attention on providing

an appropriate level of security protections for the most sensitive information systems and data that support the critical mission and functions of HHS and is necessary to ensure these security activities are implemented fully and consistently at all levels of HHS. An effective IT Security program will decrease the number and severity of exploits of sensitive HHS information systems, including compromise of mission critical data. Maintenance and updating of infrastructure will be required Department-wide in order to proactively identify and address vulnerabilities before they are successfully exploited. This investment does not have any dependencies with other investments. Primary beneficiaries of this investment include the Operating Divisions (OPDIVs) and Staff Divisions within HHS.

2. **How does this investment close in part or in whole any identified performance gap in support of the mission delivery and management support areas? Include an assessment of the program impact if this investment isn't fully funded.**

Prior to Secure One HHS, each HHS OPDIV was responsible for many facets of their own IT Security. Utilizing a risk based approach to security, the HHS Cybersecurity Program worked to integrate and focus priority attention on providing an appropriate level of security protections for the most sensitive information systems and data that support the critical mission and functions of HHS. The Program also continues to ensure that security policies and processes are in place to support compliance with the requirements of federal laws and compliance with OMB and National Institute of Standards and Technology (NIST) guidance related to IT security and privacy. In FY 2012 and FY 2013, the Department will shift emphasis to efforts that will enhance the automation of the continuous security monitoring of our operational systems. If the investment is not fully funded, Secure One HHS will be unable to: continue to fill performance gaps, improve HHS' ability to proactively identify vulnerabilities and protect Personally Identifiable Information (PII), integrate IT security into the enterprise program lifecycle (EPLC), and ensure the implementation of security policy and procedures throughout HHS. Additionally, the program will be unable to continue to address the IT security at the OPDIVs. The lack of funding will hinder the Program from pursuing a number of high impact activities that will address and correct existing security gaps. This includes the continued staffing and sustained operation of the HHS Computer Security Incident Response Center (CSIRC), which serves to provide continuous monitoring and security incident response coordination for the Department’s computer systems and networks. The request, also includes funds to support security engineering, and ongoing maintenance and operations for the DHS Trusted Internet Connection (TIC) and Einstein initiatives, funds for a suite of Endpoint Protection Security Tools, which will be required to comply with recent guidance requiring the automated reporting of the security continuous monitoring of all HHS and OPDIV IT systems and networks.

3. **Provide a list of this investment's accomplishments in the prior year (PY), including projects or useful components/project segments completed, new functionality added, or operational efficiency achieved.**

1) Improved tactics for addressing audit findings and developed methods for improving audit request delivery and collection of quarterly FISMA report information. 2) Worked to improve system and program weakness management. 3) Update of the Department’s Policy for Information Systems Security and Privacy (IS2P) to align it with the latest NIST guidance. 4) TIC completed the required EPLC requirements for review by the HHS CIO ITIRB. 5) Established an HSPD-12 Program Office. 6) Migration of OS users from multiple Active

Directory (AD) domains to a single AD and Security domain. 7) HHS CSIRC provided OS and HHS OPDIVs with the supporting infrastructure to build secure enclaves to house management components of world class information security technologies; Initial operating capability (IOC) was achieved for the CSIRC. The Department also achieved DHS targets prescribed for the implementation of Domain Name Systems Security (DNSSEC) upgrades to our network infrastructure.

4. **Provide a list of planned accomplishments for current year (CY) and budget year (BY).**

The CY 2012 request for IT Security is $40,000,000. The planned accomplishments for the CY 2012 request include: 1) Enable the HHS IT Security Program to continue to provide management and oversight of the Department's IT Security Program 2) Ensure compliance with the requirements of FISMA 3) Review and evaluate the security posture of Office of the Secretary (OS) information systems; manage and oversee the OS IT Security Certification & Accreditation (C&A) program in accordance with the FISMA, OMB, NIST and HHS policies and procedures 4) Continue solutions for encryption, enterprise malware and content filtering, data loss prevention, vulnerability scanning software, and automated tools for FISMA reporting, and security weakness tracking 5) Sustain the security investments made in FY 2010 and FY 2011 including the FY 2011 supplemental increase 6) Continue staffing and operation of the HHS CSIRC, which serves to provide continuous monitoring and security incident response coordination for the Department's computer systems and networks 7) Complete the Design, Development, Test and Implementation Phases for the DHS TIC.
The BY 2013 request for IT Security is $40,000,000. The planned accomplishments for the BY 2013 request include: 1) Enable the HHS IT Security Program to continue to provide management and oversight of the Department's IT Security Program. 2) Ensure compliance with the requirements of FISMA. 3) Sustain the security investments made in FY 2010 and FY 2011 including the FY 2011 supplemental increase. 4) Continued staffing and sustained operation of the HHS CSIRC. 5) Support security engineering, and maintenance and operations for the DHS TIC and Einstein initiatives. 6) Funds for a suite of Endpoint Protection Security Tools, which will be required to comply with recent guidance requiring the automated reporting of the security continuous monitoring of all HHS and OPDIV IT systems and networks and also includes continued funding for OPDIV major network security infrastructure projects.

5. **Provide the date of the Charter establishing the required Integrated Program Team (IPT) for this investment. An IPT must always include, but is not limited to: a qualified fully-dedicated IT program manager, a contract specialist, an information technology specialist, a security specialist and a business process owner before OMB will approve this program investment budget. IT Program Manager, Business Process Owner and Contract Specialist must be Government Employees.**

2010-09-24

Section C: Summary of Funding (Budget Authority for Capital Assets)

1.

Table I.C.1 Summary of Funding

	PY-1 & Prior	PY 2011	CY 2012	BY 2013
Planning Costs:	$0.0	$0.0	$0.0	$0.0
DME (Excluding Planning) Costs:	$2.0	$20.7	$1.5	$0.0
DME (Including Planning) Govt. FTEs:	$0.0	$0.0	$0.0	$0.0
Sub-Total DME (Including Govt. FTE):	$2.0	$20.7	$1.5	0
O & M Costs:	$92.0	$32.8	$33.4	$34.9
O & M Govt. FTEs:	$1.1	$3.3	$5.1	$5.1
Sub-Total O & M Costs (Including Govt. FTE):	$93.1	$36.1	$38.5	$40.0
Total Cost (Including Govt. FTE):	$95.1	$56.8	$40.0	$40.0
Total Govt. FTE costs:	$1.1	$3.3	$5.1	$5.1
# of FTE rep by costs:	9	18	30	30
Total change from prior year final President's Budget ($)		$29.6	$-0.1	
Total change from prior year final President's Budget (%)		109.62%	-0.19%	

2. If the funding levels have changed from the FY 2012 President's Budget request for PY or CY, briefly explain those changes:

The adjusted PY11 funding level totals $56,679,920. The funding adjustments included: outfit three TIC sites; establish robust capability to perform classified threat analysis; provide additional specialized resources to perform the cyber incident forensics and analysis; HSPD-12 funding to perform the assessment and transition planning for the 103 applications and systems and support the requirements of M-11-11; and integration of Logical and Physical Access Control Systems in OS.

Section D: Acquisition/Contract Strategy (All Capital Assets)

Table I.D.1 Contracts and Acquisition Strategy

Contract Type	EVM Required	Contracting Agency ID	Procurement Instrument Identifier (PIID)	Indefinite Delivery Vehicle (IDV) Reference ID	IDV Agency ID	Solicitation ID	Ultimate Contract Value ($M)	Type	PBSA ?	Effective Date	Actual or Expected End Date
Awarded	7529	HHSN276201000248U	263030501	7529							
Awarded	7529	HHSN31600010	263010050	7529							
Awarded	7555	HHSP233201000120G	GS35F4153D	4730							
Awarded	7529	HHSN276200800107P									
Awarded	7555	HHSP233200944401EC									
Awarded	7555	HHSP233200944401EC									
Awarded	7529	HHSN276200800267U	GS35F4594G	4730							
Awarded	7529	HHSN27300001	263010050	7529							
Awarded	7530	HHSM500201000060U	TIRNO99D00005	2050							
Awarded	7530	HHSM500T0006	HHSM500200900005I	7530							
Awarded	7530	HHSM500200900002U	26301D0054	7530							
Awarded	7529	HHSN276201000248U	263030501	7529							
Awarded	7529	HHSN276201100305U	263010050	7529							
Awarded	7555	HHSP233200955404JI									

2. If earned value is not required or will not be a contract requirement for any of the contracts or task orders above, explain why:
The steady state portion of ongoing program management, hardware and software renewals are monitored and reported monthly to the Department. A majority of this investment's acquisitions are Firm Fixed Price, which do not typically include EVM clauses. Previously, this investment's status was labeled as Operations and Maintenance (O&M). However, the Trusted Internet Connection (TIC) portion of this investment for FY11 and FY 12 was relabeled appropriately to Development/Modernization/Enhancement (DME). Consequently, the investment changed its status from O&M to Mixed Life Cycle. TIC is the only portion of this investment that contains DME activities and will require EVM rigor. The TIC portion has been budgeted and work is scheduled in acceptable time-phased increments as required and will be analyzed using the EVM rigor dictated in the HHS EVM Roadmap. TIC will also be monitored and reported monthly to the Department.

Exhibit 300B: Performance Measurement Report

Section A: General Information

Date of Last Change to Activities: 2012-02-27

Section B: Project Execution Data

Table II.B.1 Projects

Project ID	Project Name	Project Description	Project Start Date	Project Completion Date	Project Lifecycle Cost ($M)
289186	Trusted Internet Connection (TIC)	The Department of Health and Human Services (HHS) Trusted Internet Connections (TIC) Project was formed to comply with Office Management and Budget (OMB) Memorandum M-08-05, “Implementation of Trusted Internet Connections”. The purpose of the TIC program is to optimize individual external connections, including Internet Points of Presence (PoP) currently in use by the federal government. The TIC Initiative establishes a basis for consolidated infrastructure to achieve interoperability and communication among operating divisions. In response to this initiative, HHS will adopt a network and security architecture that complies with the Department of Homeland Security (DHS) TIC requirements and reduces the total number of external connections to include Internet, inter-agency, partner,			

Table II.B.1 Projects

Project ID	Project Name	Project Description	Project Start Date	Project Completion Date	Project Lifecycle Cost ($M)
		contractor, educational, health and research connectivity. Once implemented, the TIC environment will improve HHS's incident response capability; reduce the number of external connection points within HHS; and provide centralized monitoring of HHS network security controls. HHS TIC aligns with the HHS 2007-2012 Strategic Plan for IT infrastructure consolidation. This strategy employs the sharing and reuse of common, standards-based materials and programs that support the business of computer technology.			

Activity Summary

Roll-up of Information Provided in Lowest Level Child Activities

Project ID	Name	Total Cost of Project Activities ($M)	End Point Schedule Variance (in days)	End Point Schedule Variance (%)	Cost Variance ($M)	Cost Variance (%)	Total Planned Cost ($M)	Count of Activities
289186	Trusted Internet Connection (TIC)							

Key Deliverables

Project Name	Activity Name	Description	Planned Completion Date	Projected Completion Date	Actual Completion Date	Duration (in days)	Schedule Variance (in days)	Schedule Variance (%)
289186	289186: Planning Phase		2010-09-30	2010-09-30	2010-09-30	364	0	0.00%
289186	289186: Requirements Phase		2011-04-20	2011-04-20	2011-04-20	232	0	0.00%
289186	289186: Design Phase		2011-10-30	2011-09-30	2011-09-01	366	59	16.12%

Key Deliverables

Project Name	Activity Name	Description	Planned Completion Date	Projected Completion Date	Actual Completion Date	Duration (in days)	Schedule Variance (in days)	Schedule Variance (%)
289186	289186: Contractor Support for Development Phase Activities		2012-02-14	2012-02-14		183	-199	-108.74%
289186	289186: Contractor Support for Test Phase Activities		2012-03-31	2012-03-31		151	-153	-101.32%

Section C: Operational Data

Table II.C.1 Performance Metrics

Metric Description	Unit of Measure	FEA Performance Measurement Category Mapping	Measurement Condition	Baseline	Target for PY	Actual for PY	Target for CY	Reporting Frequency
Asset management: Percentage of IT assets that provide detailed asset inventory information e.g. IP address, machine name, OS, patch level, using security continuous monitoring automated tools.	%	Technology - Quality Assurance	Over target	51.000000	60.000000	71.000000	95.000000	Quarterly
Configuration management: Percentage of IT assets covered by an automated capability that provides visibility at the Department/OPDIV level into asset system security configuration information (e.g. comparison of agency baselines to installed configurations).	%	Customer Results - Service Quality	Over target	46.000000	60.000000	32.000000	95.000000	Quarterly
Vulnerability management: Percentage of IT assets covered by automated vulnerability management, using security continuous monitoring automated tools.	%	Process and Activities - Security and Privacy	Over target	64.000000	78.000000	41.000000	95.000000	Quarterly
Boundary protection: Percentage of HHS	%	Mission and Business Results - Support	Over target	0.000000	100.000000	0.000000	100.000000	Quarterly

Table II.C.1 Performance Metrics

Metric Description	Unit of Measure	FEA Performance Measurement Category Mapping	Measurement Condition	Baseline	Target for PY	Actual for PY	Target for CY	Reporting Frequency
network connections to the Internet in compliance with TIC implementation requirements.		Delivery of Services						
FISMA System Inventory Compliance: Percentage of systems with current Security Authorization to Operate (ATO)	%	Technology - Reliability and Availability	Over target	90.000000	99.000000	89.000000	99.000000	Monthly